UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/538,449	06/10/2005	Pim T Tuyls	NL02 1343 US	3797

65913 7590 01/16/2009

NXP, B.V.
NXP INTELLECTUAL PROPERTY DEPARTMENT
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
SU, SARAH	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
01/16/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary	Application No.	Applicant(s)	
	10/538,449	TUYLS ET AL.	
	Examiner	Art Unit	
	Sarah Su	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 October 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *4-13,15,16,18-22 and 27-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *4-10* is/are allowed.

6)☒ Claim(s) *11-13,15,16,18-22 and 27-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 June 2005* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/8/08*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. Amendment A, received on 8 October 2008, has been entered into record. In this amendment, claims 4, 6, 10-13, 15-16, and 18-22 have been amended, claims 1-3, 14, 17, and 23-26 have been cancelled, and claims 27-30 have been added.

2. Claims 4-13, 15-16, 18-22, and 27-30 are presented for examination.

Response to Arguments

3. Regarding the objections to the claims, the applicant has submitted amendments, and the examiner hereby withdraws the objection.

4. Applicant's arguments with respect to claim 10 have been fully considered and are persuasive. The rejection of 8 July 2008 has been withdrawn.

5. Applicant's arguments with respect to claims 11-13, 15-16, and 18-22, filed 8 October 2008 have been fully considered but they are not persuasive.

As to claims 11, 19, 20, and 22, it is argued by the applicant that the equation in Naccache is not the same equation as the Montgomery e^{th} power of a random number r. The examiner respectfully disagrees. Naccache discloses $T=r^v \bmod n$, where r is a random number (page 4, line 19). It is also disclosed in the applicant's specification that the Montgomery representation of $z_m=zR \bmod n$ and that modular multiplication is given by $a_m \times_m b_m = a_m b_m R^{-1} \bmod n$ (page 7, lines 5-6, 10-12).

As to claims 18 and 21, it is argued by the applicant that Naccache does not disclose providing to the verifier device a value $v=s^2$ being the Montgomery multiplication of the secret number s. The examiner respectfully disagrees. It is noted

that the limitations of claim 4 are narrower than those of claims 18 and 21. Naccache discloses that the prover computes and sends $U=r*B^d \bmod n$ to a verifier (page 4, line 23), where U represents the Montgomery square v and B represents the secret number s based on the modular multiplication discussed above.

As to claims 15 and 16: In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., x_m as the Montgomery representation of the Montgomery square of) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The examiner notes that the applicant's specification discloses modular multiplication as using the $\times_m$ notation (page 7, line 12), which is the same notation used in claims 15 and 16.

Information Disclosure Statement

6. The information disclosure statement (IDS) submitted on 8 October 2008 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Drawings

7. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 302, 303 (Figure 3).

Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

8. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: The computer program product (claim 27, line 1), computer program code means (claim 27, line 2; claim 28, line 2; claim 29, line 2; claim 30, line 2), and computer program (claim 28, line 1; claim 30, line 1) have not been described in the specification.

Claim Rejections - 35 USC § 101

9. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 27-30 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are drawn to a computer program per se. Computer programs claimed as computer listings per se are abstract instructions Computer programs are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed elements of a computer which permit the computer program's functionality to be realized. As such, these claims are not directed to one of the statutory categories of invention (See MPEP 2106.01), but are directed to nonstatutory functional descriptive material.

Please note that computer programs embodied on a computer readable medium or other structure, which would permit the functionality of the program to be realized, would be directed to a product and be within a statutory category of invention, so long as the computer readable medium is not disclosed as non-statutory subject matter per se (electromagnetic signals or carrier waves).

It is noted that the applicant's specification describes suitable medium as including wireless links using radio, microwave, optical, infrared, sonic, and the like (page 10, lines 20-23).

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 11-12, 15-16, 18-22, and 29-30 are rejected under 35 U.S.C. 102(b) as being anticipated by Naccache (EP 0578059 A1).

As to claims 11, 19, 20 and 22, Naccache discloses:

(i) providing to the verifier device a value s^e being a Montgomery e^{th} (i.e. d) **power of the secret number s** (i.e. B) (page 5, line 28)**;**

(ii) computing, by the prover device, a value $x=r^e$, being a Montgomery e^{th} power of r where r is a random number, and transmitting the value of x to the verifier device (page 4, line 19)**;**

(iii) selecting, by the verifier device, a challenge value c (i.e. e) **from a set {0, 1, . . . e-1} and transmitting the challenge value c to the prover device** (page 6, line 8)**;**

(iv) computing, by the prover device, a value $y = r \times_m s^c$ and transmitting the value y (i.e. U) **to the verifier device** (page 4, line 23)**;**

(v) checking, by the verifier device, the authenticity of the prover's response according to the values x, y and s^e previously received according to the challenge value c (page 6, lines 12-14)**.**

As to claim 12, Naccache discloses:

computing the values of y^e and $x \times_m s^{ec}$ and checking that they are the same (page 6, lines 12-14)**.**

As to claim 15, Naccache discloses:

means for selecting a random number, r (i.e. R) (page 3, line 20);

means for computing a Montgomery square of r to obtain $x=r^2$ (page 3, line 20);

means for transmitting x (i.e. Z) **to the verifier device** (page 3, lines 20-21);

means for receiving a challenge value, e (page 3, line 23);

means for computing a Montgomery product of $y = r \times_m s$ (page 2, line 56);

means for transmitting y to the verifier device (page 3, line 25).

As to claim 16, Naccache discloses:

means for selecting a random number, r (i.e. R) (page 3, line 20);

means for computing a Montgomery e^{th} power of r to obtain $x=r^e$ (page 5, line 28);

means for transmitting x to the verifier device (page 5, line 28);

means for receiving a challenge value, c (i.e. e) (page 6, line 8);

means for computing a Montgomery product of $y = r \times_m s$ (page 2, line 56);

means for transmitting y to the verifier device (page 4, line 23).

As to claims 18 and 21, Naccache discloses:

means for receiving a Montgomery square v (i.e. U) **of the secret number s** (i.e. B) (page 4, lines 16-17, 23);

means for receiving a Montgomery square x of a secret number r (page 4, line 19)**;**

means for transmitting a challenge value e (i.e. d) **to the prover device** (page 4, line 21)**;**

checking authenticity of a response y from the prover device, according to a Montgomery square of y verified against values of x and/or v received from the prover device according to the challenge value e (page 4, lines 25-28)**.**

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 29 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naccache.

As to claims 29 and 30, Naccache does not disclose:

a computer readable medium having thereon computer program code means adapted when said program is loaded onto a computer, to make the computer execute the method.

Naccache discloses a method of performing computations and algorithms (page 2, lines 30-32). It would have been obvious to one of ordinary skill in the art at the time the invention was made to perform computations and algorithms using a computer program on a computer readable medium since it was known in the art that computer programs are used to perform algorithms.

14. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Naccache as applied to claim 11 above, and further in view of Brickell (US Patent 7,165,181 B2).

As to claim 13, Naccache does not disclose:

repeating steps (ii) to (v) for a number of consecutive rounds to confirm the authenticity of the prover's response.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Naccache, as evidenced by Brickell. Brickell discloses a system and method for establishing trust without revealing identity, the system and method having:

repeating steps (ii) to (v) for a number of consecutive rounds to confirm the authenticity of the prover's response (col. 6, lines 29-30).

Given the teaching of Brickell, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Naccache with the teachings of Brickell by repeating the authorization procedure. Brickell recites motivation by disclosing that repeating the procedure makes

it less likely that an unauthorized or cheating prover can succeed in providing adequate proof to a challenger (col. 6, lines 66-67; col. 7, lines 1-3). It is obvious that the teachings of Brickell would have improved the teachings of Naccache by repeating the authentication procedure in order to prevent a cheating prover from successfully providing correct information to a challenger.

Allowable Subject Matter

15. Claims 4-10 are allowed.

16. The following is an examiner's statement of reasons for allowance:

As to claim 4, it was not found to be taught in the prior art of providing the Montgomery square of a secret number to a verifier, computing the Montgomery square of a random number and transmitting it to the verifier, selecting a challenge value from a set of {0,1} and sending it to the prover, computing $y = r \times_m s^e$ and sending y to the verifier, and checking the authenticity of the response.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

17. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Sarah Su/
Examiner, Art Unit 2431

/Christopher A. Revak/
Primary Examiner, Art Unit 2431